

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2005 年 10 月 27 日 (27.10.2005)

PCT

(10) 国際公開番号  
WO 2005/101220 A1

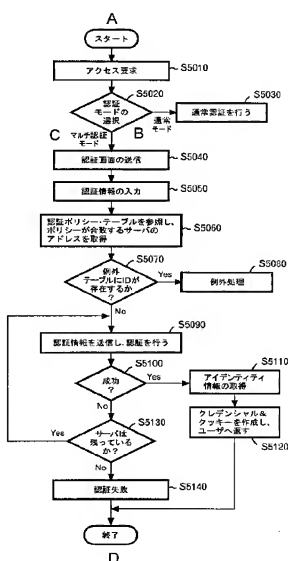
(51) 国際特許分類<sup>7</sup>: G06F 15/00, H04L 9/00 (25) 国際出願の言語: 日本語  
(21) 国際出願番号: PCT/JP2005/002143 (26) 国際公開の言語: 日本語  
(22) 国際出願日: 2005 年 2 月 14 日 (14.02.2005) (30) 優先権データ: 特願2004-099243 2004 年 3 月 30 日 (30.03.2004) JP

[続葉有]

(54) Title: USER AUTHENTICATION SYSTEM, METHOD, PROGRAM, AND RECORDING MEDIUM CONTAINING THE PROGRAM

(54) 発明の名称: ユーザ認証のためのシステム、方法、およびプログラムならびに該プログラムを記録した記録媒体

(57) Abstract: [PROBLEMS] To realize more convenient user authentication. [MEANS FOR SOLVING PROBLEMS] There is provided a user authentication system for a computing environment containing a plurality of servers which can be trusted by one another. The system includes: an authentication policy table containing authentication policy of at least one of the servers; means for receiving authentication information from a user; means for specifying at least one of the servers employing an authentication policy matched with the authentication information among the servers by using the authentication policy table; means for transmitting a signal for instructing to perform user authentication by using the authentication information, to an authentication mechanism of the server specified by the means for specifying a server; and means for permitting the user to access the computing environment if the user authentication is successful.



A START  
S5010 ACCESS REQUEST  
S5020 AUTHENTICATION MODE SELECTION  
B NORMAL MODE  
C MULTI-AUTHENTICATION MODE  
S5030 PERFORM NORMAL AUTHENTICATION  
S5040 TRANSMIT AUTHENTICATION SCREEN  
S5050 INPUT AUTHENTICATION INFORMATION  
S5060 REFERENCE AUTHENTICATION POLICY TABLE AND ACQUIRE ADDRESS  
OF SERVER WHOSE POLICY IS MATCHED  
S5070 ID EXISTS IN AN EXCEPTION TABLE?  
S5080 PERFORM EXCEPTIONAL PROCESSING  
S5090 TRANSMIT AUTHENTICATION INFORMATION AND PERFORM  
AUTHENTICATION  
S5100 SUCCESSFUL?  
S5110 ACQUIRE IDENTITY INFORMATION  
S5120 CREATE CREDENTIAL & COOKIE AND RETURN THEM TO USER  
S5130 ANY SERVER REMAINS?  
S5140 AUTHENTICATION FAILURE  
D END

(57) 要約: 【課題】 より利便性の高いユーザ認証を実現する。【解決手段】 互いに信頼関係が確立された複数のサーバを含むコンピューティング環境に対するユーザ認証を行うためのシステムであって、複数のサーバのうちの少なくとも1つの認証ポリシーを登録した認証ポリシーテーブルと、ユーザから認証情報を受ける手段と、認証ポリシーテーブルを用いて、複数のサーバから認証情報と適合する認証ポリシーを採用するサーバを少なくとも1つ特定する手段と、サーバを特定する手段によって特定されたサーバの認証機構に、認証情報を用いてユーザ認証を

[続葉有]

WO 2005/101220 A1



- (71) 出願人 (日本についてのみ): 日本アイ・ビー・エム株式会社 (IBM JAPAN, LTD.) [JP/JP]; 〒1060032 東京都港区六本木三丁目2番12号 Tokyo (JP).
- (71) 出願人 (ボツワナ, ナミビア, 日本, サン・マリノ, 米国を除く全ての指定国について): インターナショナル・ビジネス・マシーンス・コーポレーション (INTERNATIONAL BUSINESS MACHINES CORPORATION) [US/US]; 10504 ニューヨーク州アーモンク ニューオーチャードロード New York (US).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 竹日 正弘 (TAKEHI, Masahiro) [JP/JP]; 〒1060032 東京都港区六本木三丁目2番12号 日本アイ・ビー・エム株式会社内 Tokyo (JP).
- (74) 代理人: 坂口 博, 外 (SAKAGUCHI, Hiroshi et al.); 〒2428502 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社大和事業所内 Kanagawa (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:  
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明 細 書

ユーザ認証のためのシステム、方法、およびプログラムならびに該プログラムを記録した記録媒体

### 技術分野

[0001] 本発明は、一般的には、ユーザ認証技術に関し、より詳細には、連邦化されたコンピューティング環境において、ユーザを認証するシステム、方法およびプログラムに関する。

### 背景技術

[0002] 近年、多くのコンピュータ関連企業は、インターネット技術を利用してビジネス取引を自動化するためにウェブ・サービス関連技術の開発を進めている。ウェブ・サービスは、複数の企業システム間での電子商取引の効率化を実現することを目的の一つとする。より詳細には、ウェブ・サービスは、ウェブベースのアプリケーション・プログラムが自動的に関連する他のアプリケーション・プログラムを探し出すことで、複数の企業システム間の連携を実現する仕組みを提供する。

[0003] そのようなウェブ・サービスのためのセキュリティ仕様である”WS-Security”が国際ナショナル・ビジネス・マシーンズ・コーポレーション、マイクロソフト・コーポレーションおよびベリサイン・インクによって公開された(非特許文献1)。“WS-Security”では、互いに信頼関係が確立された複数のサーバを含む連邦化されたコンピューティング環境でシングル・サインオンを実現する仕組みを定義している。ここで、「信頼関係」とは、2以上のサーバのうちのいずれか1つの認証システムにおいてユーザ認証に成功したことをもって、他のサーバに対してもそのユーザを認証されたとして取り扱う場合の当該2以上のサーバの間の関係をいう。なお、前述の連邦化の仕様の一例は、“WS-Federation”として公開されている(非特許文献2)。

[0004] 背景技術では、ユーザは、複数のサーバを含む連邦化されたコンピューティング環境を利用しようとする場合、セキュリティ・トークンを取得するために複数のサーバのうちのいずれかのサーバの認証システムを使用してユーザ認証を行う。次に、取得したセキュリティ・トークンを含むSOAP(Simple Object Access Protocol)メッセー

ジに署名をした上で、ウェブ・サービスを提供するサーバにそのSOAPメッセージを送信する。SOAPメッセージを受信したサーバは、そのSOAPメッセージに含まれるセキュリティ・トークンを検証し、検証に成功したことに応じて、ユーザに対してサービスの返信をする。

[0005] 上記の”WS-Security”の仕様が正式に受理され、製品として実装されることで普及すれば、企業間システムのシームレスな連携が加速され、例えば、多数の企業システムが参加する大規模なサプライチェーン・システムが実現するだろう。

[0006] 非特許文献1:丸山宏ほか著、「Web Service Security(WS-Security)」、2002年 4月 5日、インターナショナル・ビジネス・マシーンズ・コーポレーション／マイクロソフト・コーポレーション／ベリサイン・インク発行

非特許文献2:丸山宏ほか著、「Web Service Federation Language(WS-Federation)」、2003年 7月 8日、インターナショナル・ビジネス・マシーンズ・コーポレーション／マイクロソフト・コーポレーション／ベリサイン・インク発行

発明の開示

発明が解決しようとする課題

[0007] 連邦化されたコンピューティング環境において、すべてのサーバの認証システムが同一の認証ポリシー（認証ポリシーは、指紋認証、声紋認証その他の認証形式や個々の認証形式における規約（文字数、有効期限、データサイズその他）、およびそれらの組合せを含むユーザ認証の形式の全てを含む概念である。）を採用しているのであれば、ユーザは、同一の認証情報を登録することで、いずれのサーバの認証システムを自分が使用しているのかを意識することなく、自己の「唯一の」認証情報を使用してユーザ認証を行い、連邦化されたコンピューティング環境を利用することができるだろう。

[0008] しかしながら、連邦化されたコンピューティング環境に含まれる複数のサーバの認証システムは、それぞれ異なる認証ポリシーを採用することが多い。なぜなら、連邦化されたコンピューティング環境は、独立して運用され得る複数のシステムが参加することが予定されているからである。そのような性質に起因して連邦化されたコンピューティング環境に含まれる第1のサーバと第2のサーバが異なる認証ポリシーを採用

している場合、ユーザは第1のサーバと第2のサーバそれぞれに対して、異なった認証ポリシーに適合する認証情報を設定することになる。

[0009] このようなコンピューティング環境では、ユーザは、サーバの認証システムと認証情報の対応を記憶した上で、いま自分がどの認証システムにおいて認証を試みているかを正確に意識して当該認証システムに対応する認証情報を入力することを強いられる。連邦化されたコンピューティング環境に参加するサーバの増加に比例して、ユーザが記憶すべき認証情報の数も増加するので、このオペレーションはユーザの大きな負担となる可能性がある。

[0010] そこで本発明は、上記の課題を解決することができる認証システム、認証方法、認証プログラムを提供することを目的とする。

#### 課題を解決するための手段

[0011] 上記課題を解決するために、本発明の第1の態様によれば、互いに信頼関係が確立された複数のサーバを含むコンピューティング環境に対するユーザ認証を行うためのシステムであって、複数のサーバのうちの少なくとも1つの認証ポリシーを登録した認証ポリシーテーブルと、ユーザから認証情報を受け取る手段と、認証ポリシーテーブルを用いて、複数のサーバから認証情報と適合する認証ポリシーを採用するサーバを少なくとも1つ特定する手段と、サーバを特定する手段によって特定されたサーバの認証機構に、認証情報を用いてユーザ認証を行うように命令する信号を送信する手段と、ユーザ認証が成功したことを条件として、ユーザのコンピューティング環境へのアクセスを許可する手段と、を備えたシステムが提供される。

[0012] また、本発明の第2の態様によれば、互いに信頼関係が確立された複数のサーバを含むコンピューティング環境における方法であって、複数のサーバのうちの少なくとも1つの認証ポリシーを登録した認証ポリシーテーブルを少なくとも1つ保持し、ユーザから認証情報を受け取るステップと、認証ポリシーテーブルを用いて、複数のサーバから認証情報と適合する認証ポリシーを採用するサーバを少なくとも1つ特定するステップと、サーバを特定するステップにおいて特定されたサーバの認証機構に、認証情報を用いてユーザ認証を行うように命令する信号を送信するステップと、ユーザ認証が成功したことを条件として、コンピューティング環境へのアクセスが許可されるス

テップと、を含む方法が提供される。

[0013] さらに、本発明の第3の態様によれば、互いに信頼関係が確立された複数のサーバを含むコンピューティング環境におけるプログラムであって、複数のサーバの少なくとも1つの認証ポリシーを登録した認証ポリシーテーブルを少なくとも1つ保持し、認証プログラムは、ユーザから認証情報を受けるステップと、認証ポリシーテーブルを用いて、複数のサーバから認証情報と適合する認証ポリシーを採用するサーバを少なくとも1つ特定するステップと、サーバを特定するステップにおいて特定されたサーバの認証機構に、認証情報を用いてユーザ認証を行うように命令する信号を送信するステップと、ユーザ認証が成功したことを条件として、コンピューティング環境へのアクセスが許可されるステップと、をコンピュータに実行させるプログラムが提供される。

[0014] また、本発明の第4の態様として、上述したプログラムを記録したコンピュータ可読の記憶媒体のようなコンピュータ・プログラム製品が提供される。

#### 発明の効果

[0015] 本発明によれば、連邦化されたコンピューティング環境において、より利便性の高いユーザ認証が可能となる。

#### 発明を実施するための最良の形態

[0016] 以下、本発明を実施するための最良の形態を図面に基づいて詳細に説明する。なお、本発明は多くの異なる態様で実施することが可能であり、実施の形態の記載内容に限定して解釈されるべきものではなく、また実施の形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須とは限らないことに留意されたい。また、実施の形態の説明の全体を通じて同じ要素には同じ番号を付している。

[0017] 以下の実施の形態では、主に方法およびシステムについて説明するが、当業者であれば明らかな通り、本発明はコンピュータで使用可能なプログラムとしても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムは、ハードディスク、CD-ROM、光記憶装置または磁気記憶装置等の任意のコンピュータ可読媒体に記録できる。

[0018] 図1は、本発明の実施の形態における連邦化されたコンピューティング環境1000

のシステム構成の一例を示した概念図である。連邦化されたコンピューティング環境1000は、ネットワーク200で互いに接続されたクライアント100および複数のサーバ300-1〜300-N(以下、必要に応じてサーバ300と総称する)を含んでいる。

- [0019] クライアント100は、周知のインターネットに接続可能な端末である。当業者は、そのようなクライアント100を容易に実施することができる。また、クライアント100とネットワーク200の接続は、ダイヤルアップ接続等によりISP(Internet Service Provider、図示せず)を介して行うとよい。なお、クライアント100からISPへの接続はダイヤルアップ接続に制限されるものではなく、例えば、専用線、LAN(Local Area Network)、WAN(Wide Area Network)、ADSL(Asymmetric Digital Subscriber Line)、CATV(Cable Television)を用いた常時接続により行ってもよい。
- [0020] ネットワーク200は、クライアント100、サーバ300を接続する通信経路であり、一例としてインターネットにより実現することができる。インターネットであるネットワーク200は周知の通り、TCP/IP(Transmission Control Protocol/Internet Protocol)を用いてシステム間を接続する。ネットワーク200ではグローバルアドレスまたはローカルアドレスで表されるIPアドレスによって相互に通信するシステムが特定される。
- [0021] サーバ300は、クライアント100からの要求に応じてサービスを提供するコンピュータ装置である。より詳細には、サーバ300-1〜300-Nは、周知のウェブ・サービス技術を使用して、クライアント100からのサービス要求に対して、互いに連携してウェブ・サービスを提供する。好適には、サーバ300-1〜300-Nは、前述の”WS-Federation”仕様に従って、互いに信頼関係が確立された連邦化されたコンピューティング環境1000を形成する。
- [0022] 図2は、本実施の形態におけるサーバ300の機能ブロック図である。図2の機能ブロック図に示す各要素は、後述する図11に例示したハードウェア構成を有するコンピュータにおいて、ハードウェア資源とソフトウェアを協働させることで実現することができる。
- [0023] サーバ300は、通信制御部310、ユーザ認証処理部320、アプリケーション実行部330を含む。通信制御部310は、ネットワーク200から受けたデータを、ユーザ認証

処理部320またはアプリケーション実行部330へ転送する。通信制御部310は、ユーザ認証処理部320またはアプリケーション実行部330から受けたデータを、ネットワーク200へ送出することもできる。

- [0024] ユーザ認証処理部320は、通信制御部310を通じて受けたクライアント100のユーザのアクセス要求に応じて認証処理を行う。好適には、アクセス要求は、クライアント100のウェブ・ブラウザにおいて生成され、ネットワーク200に送出されサーバ300に受信されたHTTP(HyperText Transfer Protocol)リクエストとして実装されるが、これに限定されない。ユーザ認証処理部320は、認証要求処理部321、認証情報管理部322、LDAPクライアント323、認証ポリシーテーブル324、例外IDテーブル325および認証情報LDAP326を含む。
- [0025] 認証要求処理部321は、クライアント100のユーザからのアクセス要求を解析し、アクセス要求を送信したユーザが未認証であると判定された場合は、ユーザ認証を実行する。つまり、認証要求処理部321は、認証ポリシーテーブル324を参照して、連邦化されたコンピューティング環境1000に含まれる他のサーバの認証システムと連携してユーザ認証を実行する。
- [0026] より詳細には、認証要求処理部321は、アクセス要求を送信したクライアント100のユーザが未認証であると判定されたことに応じて、認証情報の入力を促すウェブ・ページのデータをクライアント100に送信する機能を有する。また、認証要求処理部321は、認証情報入力用ウェブ・ページ使用して入力されたユーザの認証情報を受け、認証ポリシーテーブル324を使用して、当該認証情報が、連邦化されたコンピューティング環境1000に含まれる複数のサーバのうち、いずれのサーバの認証システムの認証ポリシーに適合するかを特定し、特定されたサーバの認証システムの認証機構において、認証情報を用いてユーザ認証を命令する信号を送信する機能を有する。
- [0027] さらに、認証要求処理部321は、認証情報が自身の認証ポリシーに適合すると判定された場合に、当該認証情報と、LDAPクライアント323を通じて入手した認証情報LDAP326に格納された認証情報の突き合わせを行う認証機構を有する。さらに、認証要求処理部321は、ユーザ認証が成功した場合に、クライアント100に連邦化されたコンピューティング環境1000へのアクセスを許可するセキュリティ・トークンを送



信する機能している。本実施の形態では、好適には、セキュリティ・トークンは、クレデンシャルおよびクッキーである。

- [0028] 認証情報管理部322は、連邦化されたコンピューティング環境1000における認証情報の管理を行う。好適には、認証情報管理部322は、連邦化されたコンピューティング環境1000に含まれるサーバの認証システムの認証ポリシーの認証ポリシーテーブル324への登録、更新および参照の処理を行う機能を有する。また、認証情報管理部322は、LDAPクライアント323を通じて、ユーザから受けた認証情報を認証情報LDAPへ登録する機能を有する。さらに、認証情報管理部322は、新規ユーザのユーザIDを登録する際に、同一の認証ポリシーを採用する他のサーバの認証システムに同一のユーザIDが既に登録されているかどうかを判定し、同一のユーザIDが登録されていると判定された場合に、当該ユーザIDを例外IDテーブル325に登録する機能を有する。
- [0029] LDAPクライアント323は、認証情報LDAP326へのインターフェースを提供する。より詳細には、LDAPクライアント323は、サーバ300のプログラム・コンポーネントまたは他のコンピュータからの認証情報LDAP326へのアクセスを制御する機能を有する。LDAPクライアント323は、少なくとも、認証情報管理部322から受けた認証情報を認証情報LDAP326へ登録することができ、また、認証要求処理部321等の要求に応じて認証情報LDAP326に登録されている認証情報を取り出すことができる。
- [0030] 認証ポリシーテーブル324は、連邦化されたコンピューティング環境1000に含まれる各サーバの認証システムの認証ポリシーを登録するテーブルである。
- [0031] 図9は、本発明の実施形態における認証ポリシーテーブル324の一例を示した図である。認証ポリシーテーブル324には、連邦化されたコンピューティング環境1000に含まれるサーバの一部または全部のアドレス・ロケーション(好適には、当該サーバのURLアドレス)が、認証ポリシーと関連付けられて登録されている。図9に例示する認証ポリシーテーブル324では、第一列に認証ポリシーが登録され、第二列に第一列の認証ポリシーを採用するサーバのアドレスが登録されている。
- [0032] なお、認証ポリシーテーブル324には、連邦化されたコンピューティング環境1000に含まれるすべてのサーバのアドレス・ロケーションおよび認証ポリシーが登録されるこ

とが好ましい。しかし、後述するように、本実施形態のユーザ認証は、認証ポリシーテーブル324にアドレス・ロケーションおよび認証ポリシーが登録されたサーバのいずれかにおいてユーザ認証が成功したことに応じて連邦化されたコンピューティング環境1000へのアクセスを許可するものであるので、連邦化されたコンピューティング環境1000に含まれるサーバのアドレス・ロケーションおよび認証ポリシーが登録されていなくても本実施形態のユーザ認証は動作可能であることに留意されたい。

[0033] さらに、本発明の実施形態における認証ポリシーテーブル324では、同一の認証ポリシーを採用するサーバが複数存在する場合に、どのサーバの認証システムからユーザ認証の処理を行うかを示すプライオリティがサーバアドレスと関連付けて登録される。プライオリティの値は、システム管理者がマニュアルで入力をしてよいし、認証システムに登録されているユーザ数の多い順で値を割り振るなど、自動的に決定してもよい。

[0034] より具体的には、本発明の実施形態における認証ポリシーテーブル324には、ユーザIDが「アルファベット3文字＋数字3文字」かつパスワードが「アルファベット4文字」の認証ポリシーを採用する3つのサーバ(アドレスは”server300-1.com”、”server300-2.com”、”server300-3.com”)が登録されている。また、ユーザIDが「アルファベット8文字」かつパスワードが「任意」の認証ポリシーを採用する2つのサーバ(アドレスは”server300-4.com”、”server300-5.com”)も登録されている。

[0035] さらに、認証ポリシーテーブル324には、「指紋認証」かつ指紋認証のバイナリデータのサイズが「100bytes」の認証ポリシーを採用する2つのサーバ(アドレスは”server300-6.com”、”server300-7.com”)および「声紋認証」かつ声紋認証のバイナリデータのサイズが「200bytes」の認証ポリシーを採用する1つのサーバ(アドレスは”server300-8.com”)も登録されている。

[0036] 例外IDテーブル325は、連邦化されたコンピューティング環境1000に含まれる各サーバの認証システムの間で同一のユーザIDを別のユーザが使用している場合に、当該ユーザIDを例外IDとして登録するテーブルである。

[0037] 図10は、本発明の実施形態における例外IDテーブル325の一例を示した図である。例外IDテーブル325には、連邦化されたコンピューティング環境1000に含まれ

るサーバの一部または全部のアドレス・ロケーション(好適には、当該サーバのURLアドレス)が、例外IDと関連付けられて登録されている。図10に例示する例外IDテーブル325では、第一列にサーバアドレスが登録され、第二列に第一列のサーバの認証システムの例外IDが登録されている。

[0038] アプリケーション実行部330は、認証されたユーザのサービス要求を実現するために、クライアント100および／または連邦化されたコンピューティング環境1000に含まれるサーバからの要求に応じて、種々のアプリケーション・プログラムを実行する。好適には、アプリケーション実行部330によって実行されるアプリケーション・プログラムは、ウェブベースのアプリケーション・プログラムとして実現される。本発明の実施の形態においては、アプリケーションA(331)、アプリケーションB(332)、アプリケーションC(333)およびアプリケーションD(334)の4種類のアプリケーションを実行することができるようになっている。

[0039] 図3は、複数のサーバ間の信頼関係を確立する動作フローを示したフローチャートである。本実施の形態においては、複数のサーバ300-1〜300-Nが互いに信頼関係を確立する場合、まず、サーバ300-1が、図3に記載した動作フローに従ってまだ信頼関係の確立されていないサーバ300-2〜300-Nとの信頼関係を確立する。次に、サーバ300-2が、同様に図4に記載した動作フローに従って、まだ信頼関係の確立されていないサーバ300-3〜300-Nとの信頼関係を確立する。これをサーバ300-(N-1)まで繰り返すことで、複数のサーバ300-1〜300-Nの互いの信頼関係がすべて確立され、連邦化されたコンピューティング環境1000が形成される。

[0040] 以下に、サーバ300-1がサーバ300-2〜300-Nとの間で信頼関係を確立する場合を例として、図3に示す動作フローを詳細に説明する。最初に、サーバ300-1は、自己の認証ポリシーを認証ポリシーテーブル324へ登録する(S3010)。次に、周知のPKI(Public Key Infrastructure)方式に従って電子証明書を交換することで、サーバ300-1とサーバ300-2の間の信頼関係を確立する(S4020)。

[0041] 次に、サーバ300-1は、S3020において信頼関係を確立した相手方のサーバであるサーバ300-2の認証ポリシーを入手する。具体的には、サーバ300-1は、サーバ300-2にローカルに存在するサーバ300-2の管理者が作成した認証ポリシーを記

述したプロファイル・テーブルにアクセスすることで、サーバ300-2の認証ポリシーを入手する。そして、入手したサーバ300-2の認証ポリシーを認証ポリシーテーブル324に登録した上で(S3030)、自己の認証ポリシーと相手方サーバ300-2の認証ポリシーが同一かどうかを判定する(S3040)。サーバ300-1とサーバ300-2の認証ポリシーが同一でないと判定された場合は、信頼関係をまだ確立していないサーバが存在するかどうかを判定するためにNOの矢印からS3090へ進む。

[0042] S3040においてサーバ300-1とサーバ300-2の認証ポリシーが同一と判定された場合は、YESの矢印からS3050へ進み、サーバ300-1とサーバ300-2の認証情報LDAP326に同一のユーザIDが存在するかどうかを調べる。S3050においてサーバ300-1とサーバ300-2の認証情報LDAP325に同一のユーザIDが存在しないと判定された場合は、信頼関係をまだ確立していないサーバが存在するかどうかを判定するためにNOの矢印からS3090へ進む。

[0043] S3050においてサーバ300-1とサーバ300-2の認証情報LDAPに同一のユーザIDが存在すると判定された場合は、YESの矢印からステップ3060へ進み、図6に示す例外ID登録確認画面を、サーバ間の信頼関係を確立しようとしているシステム管理者の操作する端末へ表示する。本実施の形態では、サーバ300-1とサーバ300-2の双方に、“ABC001”というユーザIDが登録されていたとして、システム管理者に当該ユーザIDが同一のユーザが使用するものかどうかについて確認を促している。なお、例外ID登録確認画面には、システム管理者に確認のヒントを提示するために、サーバ名、ユーザIDと関連付けて登録名(サーバ300-1のユーザID“ABC001”に対する登録名として“Tanaka Taro”、サーバ300-2のユーザID“ABC001”に対する登録名として“Hirota Keisuke”)が表示される。

[0044] 次に、S3070に進み、システム管理者が、例外ID確認画面に表示されたユーザIDが、サーバ300-1とサーバ300-2で異なるユーザが使用していると判断した場合、システム管理者は、例外ID確認画面で“登録する”ボタンを押すことになる。“登録する”ボタンが押されたことに応じてフローはS3080に進み、当該ユーザIDは、例外IDテーブル325に登録される。その後、信頼関係をまだ確立していないサーバが存在するかどうかを判定するためにNOの矢印からS3090へ進む。

- [0045] S3070において、システム管理者が、例外ID確認画面に表示されたユーザIDが、サーバ300-1とサーバ300-2で同一のユーザが使用していると判断した場合、ユーザは例外ID確認画面で“登録しない”ボタンを押すことになる。“登録しない”ボタンが押されたことに応じて、フローは、信頼関係をまだ確立していないサーバが存在するかどうかを判定するためにNOの矢印からS3090へ進む。
- [0046] S3090では、サーバ300-1がまだ信頼関係を確立していないサーバがあるかどうか判定される。S3090でまだ信頼関係を確立していないサーバがあると判定された場合は、フローはS3030へ戻り、まだ信頼関係を確立していないサーバとS3030～S3080のステップを実行することでサーバ300-1は、すべての他のサーバ300-2～300-Nと信頼関係を確立することとなる。S3090でまだ信頼関係を確立していないサーバがもう存在しないと判定された場合は、YESの矢印に進み、フローは終了する。
- [0047] 上記は、サーバ300-1が、他のサーバ300-2～300-Nと信頼関係を確立することについて説明した。同様の処理を300-2～300-Nについても実行することで、サーバ300-1～300-Nの間で互いに信頼関係を確立した連邦化されたコンピューティング環境1000が形成される。
- [0048] 図4は、新規ユーザ認証情報の登録の動作フローを示したフローチャートである。以下に、既に複数のサーバ300-1～300-Nで互いに信頼関係が確立された連邦化されたコンピューティング環境1000に参加するサーバ300-1の認証システムにおいて、新規ユーザ認証情報を登録する流れを、図4を参照して詳細に説明する。なお、他のサーバ300-2～300-Nの認証システムにおいて新規ユーザ認証情報を登録する流れも同様の処理で実現可能であることに留意されたい。
- [0049] まず、ユーザの操作するクライアント100から新規認証情報を受け付ける(S4010)。なお、S4010では、サーバ300-1は、サーバ300-1の管理者が作成した認証ポリシーを記述したプロファイル・テーブルを使用して、新規認証情報が自己の認証ポリシーに適合しているかどうかの検証も行っている。次に、自己の認証情報LDAP326に、クライアント100から受けた認証情報に含まれるユーザIDと同一のユーザIDが存在するかどうかを判定する(S4020)。S4020で同一のユーザIDが存在すると判定さ

れた場合は、同一のサーバの認証システムでは同一のユーザIDが存在をすることは許されないので、別の認証情報をユーザから受け付けるためにYESの矢印からS4010へ戻り、再度新規ユーザ認証情報を受け付ける。S4020で同一のユーザIDが存在しないと判定された場合は、NOの矢印からS4030へ進む。

[0050] S4030では、サーバ300-1は、自己の記憶装置に記憶されている認証ポリシーテーブルを用いて、連邦化されたコンピューティング環境1000に存在する自己と同一の認証ポリシーを採用する認証システムを持つサーバを特定する。次に、S4030で自己と同一の認証ポリシーを採用する認証システムを持つサーバとして特定されたサーバのうちの一つの認証情報LDAP326に新規ユーザ認証情報に含まれるユーザIDと同一のユーザIDが存在するかどうかを判定する(S4040)。

[0051] S4040において、S4030で特定されたサーバのうちの一つの認証情報LDAP326に同一のユーザIDが存在しないと判定された場合は、他にS4030で特定された300-1と同一の認証ポリシーを採用するサーバが存在するかどうかを判定するためにNOの矢印からS4080へ進む。

[0052] S4040において、S4030で特定されたサーバのうちの一つの認証情報LDAP326に同一のユーザIDが存在すると判定された場合は、YESの矢印からS4050へ進み、図6に示す例外ID登録確認画面を、認証情報を登録しようとしているユーザが操作するクライアントへ表示する。例外ID登録確認画面については、図3の説明において既にしたので、ここでは詳細には説明しない。

[0053] 次に、S4060に進み、認証情報を登録しようとするユーザが、例外ID確認画面に表示されたユーザIDを自分が使用しているものではないと判断した場合、ユーザは例外ID確認画面で“登録する”ボタンを押すことになる。“登録する”ボタンが押されたことに応じてフローはS4070に進み、当該ユーザIDは、例外IDテーブル325に登録される。その後、他にS4030で特定された300-1と同一の認証ポリシーを採用するサーバが存在するかどうかを判定するためにNOの矢印からS4080へ進む。

[0054] なお、S4060において、認証情報を登録しようとするユーザが、例外ID確認画面に表示されたユーザIDを自分が使用しているものであると判断した場合、ユーザは例外ID確認画面で“登録しない”ボタンを押すことになる。“登録しない”ボタンが押され

たことに応じて、他にS4030で特定された300-1と同一の認証ポリシーを採用するサーバが存在するかどうかを判定するためにYESの矢印からS4080へ進む。

[0055] S4080では、S4030で特定されたサーバ300-1と同一の認証ポリシーを採用するサーバがまだ残っているかが判定される。S4080でまだ同一の認証ポリシーを採用するサーバが残っていると判定された場合は、フローはS4040へ戻り、残っているサーバとS4040〜S4070のステップを実行することで、サーバ300-1は、必要な情報を例外IDテーブルに登録する。S4080でまだ同一の認証ポリシーを採用するサーバが残っていないと判定された場合は、NOの矢印からS4090へ進み、サーバ300-1は、新規ユーザ認証情報を自己の認証情報LDAP326に登録する。

[0056] 図5は、本発明の実施形態におけるユーザ認証の流れを示したフローチャートである。以下、未認証のユーザの操作するクライアント100から連邦化されたコンピュータ環境1000に含まれる複数のサーバの一つであるサーバ300-1に対してアクセス要求があった場合のユーザ認証の流れを図5のフローチャートに従って詳細に説明する。なお、他のサーバ300-2〜300-Nの認証システムにおいてユーザ認証を行う場合も同様の処理で実現可能であることに留意されたい。

[0057] サーバ300-1は、ユーザからアクセス要求を受ける(S5010)。そして、アクセス要求にセキュリティ・トークンが含まれるかどうかを調査することによって当該アクセス要求を発したユーザが未認証であると判定したサーバ300-1は、ユーザの操作するクライアントに、図7に示す認証モード選択画面のデータを送信することで、ユーザに認証モードの選択を促す(S5020)。ユーザが、図7に例示する認証モード選択画面に“はい”のボタンを押し、マルチ認証モードを選択した場合は、処理はS5040へ進む。なお、ユーザが図7に例示する認証モード選択画面に“いいえ”のボタンを押し、通常認証モードが選択した場合は、処理はS5030へ進み、認証ポリシーテーブルを使わない通常認証でユーザ認証が行われる。通常認証は、周知であるのでここでは詳細には説明されない。

[0058] 次に、サーバ300-1は、図8に示すマルチ認証モードで用いられる認証画面のデータをユーザのクライアントに送信する(S5040)。認証画面のデータを受けたユーザは、認証情報を入力する(S5050)。クライアントは、入力された認証情報をサーバ3

00-1へ送信する。

- [0059] より詳細には、ユーザIDを使用してユーザ認証を行う場合は、ユーザは、図8に示す認証情報入力画面の第一行にキーボードを操作することでユーザIDを入力する。ユーザIDを使用せずにユーザ認証を行う場合は、ユーザは、第一行の“使用しない”のチェックボックスをチェックする。また、パスワードを使用してユーザ認証を行う場合は、ユーザは、図8に示す認証画面の第二行にキーボードを操作することでパスワードを入力する。パスワードを使用せずにユーザ認証を行う場合は、ユーザは、第二行の“使用しない”のチェックボックスをチェックする。指紋認証、声紋認証などテキストデータ以外(すなわち、バイナリデータ)を使用してユーザ認証を行う場合は、ユーザは、図8に示す認証画面の第三行の“使用しない”のチェックボックスをチェックせずに“OK”ボタンを押し、続けてバイナリデータの入力(例えば、指紋認証に対して指紋データ入力パッドに指を置く、声紋認証に対してはマイクに向かって発声するなど)を行う。パスワードを使用せずにユーザ認証を行う場合は、ユーザは、第二行の“使用しない”のチェックボックスをチェックする。
- [0060] 処理はS5050に進み、サーバ300-1は、自己の認証ポリシーテーブルを参照し、ユーザが入力した認証情報と適合する認証ポリシーを採用する1以上のサーバのアドレスを取得する(S5060)。例えば、サーバ300-1が図9の認証ポリシーテーブルを使用し、認証情報にユーザIDが“XYZ001”、パスワードが“WXYZ”が含まれる場合は、ユーザIDが「アルファベット3文字+数字3文字」かつパスワードが「アルファベット4文字」の認証ポリシーに適合するので、サーバ300-1は、3つのアドレス“server300-1.com”、“server300-2.com”、“server300-3.com”を取得する。
- [0061] 次に、サーバ300-1は、ユーザからの認証情報に含まれるユーザIDが例外IDテーブルに登録されているかどうかを、S5060で取得されたアドレスの示すサーバに対して問合せを行うことで判定する(S5070)。認証情報に含まれるユーザIDが例外IDテーブルに登録されていると判定された場合は、YESの矢印からS5080へ進み例外処理が行われる。例外IDテーブルに登録されているユーザIDは、いずれの認証システムにおいてユーザ認証すべきかを判別することができないので、例外処理では、サーバ300-1は、ユーザのクライアントに「このユーザIDは例外IDですので、マ



ルチ認証モードを使用することはできません。通常認証にてユーザ認証を行ってください。」というメッセージを返し、処理を終了する。

[0062] S5070において、ユーザからの認証情報に含まれるユーザIDがいずれかのサーバの例外IDテーブルにも登録されてないと判定された場合は、NOの矢印からS5090へ進む。S5090では、サーバ300-1は、S5060において取得したアドレスを使用して、認証ポリシーの合致するサーバに認証情報を送信し、認証情報を受信したサーバの認証機構を使用してユーザ認証を行う。好適には、サーバ300-1は、いずれのサーバからユーザ認証を行うかを、認証ポリシーテーブル中のプライオリティの値に従って決定する。例えば、サーバ300-1が図9の認証ポリシーテーブルを使用し、S5070においてサーバ300-1が3つのアドレス”server300-1.com”、”server300-2.com”、”server300-3.com”を取得した場合は、プライオリティの値が最も高い”server300-1.com”の認証システムがユーザ認証を最初に試みることとなる。

[0063] 処理はS5100へ進み、ユーザ認証が成功したと判定された場合は、ユーザ認証を行ったサーバは、アイデンティティ情報を取得し(S5110)、取得したアイデンティティ情報を使用して、クレデンシャルおよびクッキーを作成し、ユーザに返信する(S5120)。なお、クレデンシャルおよびクッキーの作成およびユーザへの返信は、ユーザ認証を行ったサーバからユーザ認証が成功した旨の通知を受けたサーバ300-1が行ってもよい。そして、ユーザは受信したクレデンシャルおよびクッキーを使用して、連邦化されたコンピューティング環境1000にアクセスをすることが許可され、認証処理は終了する。

[0064] なお、本発明の実施形態では、ユーザに連邦化されたコンピューティング環境へのアクセスを許可するために、クレデンシャルおよびクッキーを使用する態様によって説明をした。しかし、クレデンシャルおよびクッキーの代替としてURLエンコーディング、SAMLトークンのような他のいかなる公知の認証技術も使用可能であることは当業者には自明である。

[0065] S5100でユーザ認証が失敗したと判定された場合は、S5060で特定されたユーザの認証情報に認証ポリシーが適合するサーバが残っているかどうか判定される(S6130)。S5130において、まだS5060で特定されたユーザの認証情報に認証ポリ

シーに適合するサーバが残っていると判定された場合は、フローはS5090へ戻り、他の残っているサーバに対してS5090以降の処理を行うことで、再びユーザ認証を試みることとなる。前述のサーバ300-1が図9の認証ポリシーテーブルを使用し、S5070においてサーバ300-1が3つのアドレス”server300-1.com”、”server300-2.com”、”server300-3.com”を取得した場合は、既に”server300-1.com”の認証システムによる認証は失敗したので、サーバ300-1は、プライオリティの値が次に高い”server300-2.com”の認証システムがユーザ認証を最初に試み、それも失敗した場合は、”server300-3.com”の認証システムがユーザ認証を試みることとなる。

- [0066] S5130で特定されたユーザの認証情報に認証ポリシーに適合するサーバが残っていない、すなわちすべてのサーバにおいて認証が失敗したと判定された場合は、フローはS5140へ進み、認証失敗としてユーザは連邦化されたコンピューティング環境1000へのアクセスを許可されないこととなり、認証処理は終了する。
- [0067] 図11は、本発明の実施の形態において使用されるサーバ300を実現するために好適なコンピュータ装置のハードウェア構成を例示する図である。サーバ300は、中央処理装置(CPU)1とメインメモリ4を含んでいる。CPU1とメインメモリ4は、バス2を介して、補助記憶装置としてのハードディスク装置13と接続されている。また、フレキシブルディスク装置20、MO装置28、CR-ROM装置26、29などのリムーバブルストレージ(記録メディアを交換可能な外部記憶システム)が関連するフレキシブルディスク・コントローラ19、IDEコントローラ25、SCSIコントローラ27などを介してバス2へ接続されている。
- [0068] フレキシブルディスク装置20、MO装置28、CR-ROM装置26、29などのリムーバブルストレージには、それぞれフレキシブルディスク、MO、CD-ROMなどの記憶媒体が挿入され、このフレキシブルディスク等やハードディスク装置13、ROM14には、オペレーティング・システムと協働してCPU等に命令を与え、本発明を実施するためのコンピュータ・プログラムのコードを記録することができる。メインメモリ4にロードされることによってコンピュータ・プログラムは実行される。コンピュータ・プログラムは圧縮し、また複数に分割して複数の媒体に記録することもできる。
- [0069] サーバ300は、さらに、ユーザ・インターフェイス・ハードウェアとして、マウス等のポ

インテイング・デバイス7、キーボード6や視覚データをユーザに提示するためのディスプレイ12を有することができる。また、パラレルポート16を介してプリンタ(図示せず)と接続することや、シリアルポート15を介してモデム(図示せず)を接続することが可能である。サーバ300は、シリアルポート15及びモデムを介し、また、通信アダプタ18(イーサネット(R)・カードやトークンリング・カード)等を介してネットワークに接続し、他のコンピュータ等と通信を行うことが可能である。

[0070] スピーカ23は、オーディオ・コントローラ21によってD/A変換(デジタル/アナログ変換)された音声信号をアンプ22を介して受け取り、音声として出力する。また、オーディオ・コントローラ21は、マイクロフォン24から受け取った音声情報をA/D変換(アナログ/デジタル変換)し、システム外部の音声情報をシステムに取り込むことを可能にしている。

[0071] 以上の説明により、本発明の実施の形態におけるサーバ300は、メインフレーム、ワークステーション、通常のパーソナルコンピュータ(PC)等の情報処理装置、または、これらの組み合わせによって実現されることが容易に理解されるであろう。ただし、これらの構成要素は例示であり、そのすべての構成要素が本発明の必須構成要素となるわけではない。

[0072] 特に、ここで説明したハードウェア構成のうち、フレキシブルディスク装置20、MO装置28、CR-ROM装置26、29などのリムーバブルストレージ、パラレルポート16、プリンタ、シリアルポート15、モデム、通信アダプタ18、スピーカ23、オーディオ・コントローラ21、アンプ22、マイクロフォン24などはなくても、本発明の実施の形態は実現可能であるので、本発明の実施の形態におけるサーバ300に含めなくともよい。

[0073] 本発明の実施に使用されるサーバ300の各ハードウェア構成要素を、複数のマシンを組み合わせ、それらに機能を配分し実施する等の種々の変更は当業者によって容易に想定され得るものであり、それらの変更は、当然に本発明の思想に包含される概念である。

[0074] サーバ300は、オペレーティング・システムとして、マイクロソフト・コーポレーションが提供するWindows(R)オペレーティング・システム、インターナショナル・ビジネス・マシーンズ・コーポレーションが提供するAIX、アップル・コンピュータ・インコーポレイ

テッドが提供するMacOS、あるいはLinuxなどのGUIマルチウィンドウ環境をサポートするものを採用することができる。

[0075] サーバ300は、オペレーティング・システムとして、インターナショナル・ビジネス・マシーンズ・コーポレーションが提供するPC-DOS、マイクロソフト・コーポレーションが提供するMS-DOSなどのキャラクタ・ベース環境のもの採用することもできる。さらに、サーバ300は、インターナショナル・ビジネス・マシーンズ・コーポレーションが提供するOS/Open、Wind River Systems, Inc. のVx WorksなどのリアルタイムOS、Java (R) OSなどのネットワーク・コンピュータに組み込みオペレーティング・システムを採用することもできる。

[0076] 以上から、サーバ300は、特定のオペレーティング・システム環境に限定されるものではないことを理解することができる。サーバ300-1〜300-Nはそれぞれ異なるオペレーティング・システム環境で動作するようにしてもよいことは勿論である。

[0077] 以上、本実施の形態によれば、ユーザは、連邦化されたコンピューティング環境1000のいずれかのサーバの認証システムに対するいずれかの認証情報を入力することで、サーバの認証システムと認証情報の対応を記憶することなく、また、いま自分がどの認証システムにおいて認証を試みているかを正確に意識することなくユーザ認証を受けることが可能となる。

[0078] また、本実施の形態では、ユーザから受けた認証情報に適合する認証ポリシーを採用するサーバの認証システムにおいてのみユーザ認証を行うので、高速なユーザ認証が実現される。

[0079] 以上、本発明によれば、連邦化されたコンピューティング環境において、より利便性の高いユーザ認証を実現できることが容易に理解できる。

[0080] 以上、本発明の実施の形態を用いて説明したが、本発明の技術範囲は上記実施の形態に記載の範囲には限定されない。上記の実施の形態に、種々の変更または改良を加えることが可能であることが当業者に明らかである。従って、そのような変更または改良を加えた形態も当然に本発明の技術的範囲に含まれる。

#### 図面の簡単な説明

[0081] [図1]本発明の実施の形態の連邦化されたコンピューティング環境100のシステム構

成の一例を示した概念図である。

[図2]本発明の実施形態におけるサーバ300の機能ブロック図である。

[図3]本発明の実施形態におけるサーバ間の信頼関係を確立する動作フローを示したフローチャートである。

[図4]本発明の実施形態における新規ユーザ認証情報の登録の動作フローを示したフローチャートである。

[図5]本発明の実施形態におけるユーザ認証の動作フローを示したフローチャートである。

[図6]本発明の実施形態における例外ID登録確認画面のイメージを示した図である。  
。

[図7]本発明の実施形態における認証モード選択画面のイメージを示した図である。

[図8]本発明の実施形態における認証情報入力画面のイメージを示した図である。

[図9]本発明の実施形態における認証ポリシーテーブル324の一例を示した概念図である。

[図10]本発明の実施形態における例外IDテーブル325の一例を示した概念図である。

[図11]本発明の実施形態におけるサーバ300として機能するコンピュータのハードウェア構成の一例を示した図である。

## 請求の範囲

- [1] 互いに信頼関係が確立された複数のサーバを含むコンピューティング環境に対するユーザ認証を行うためのシステムであって、
- 前記複数のサーバのうちの少なくとも1つの認証ポリシーを登録した認証ポリシーテーブルと、
- ユーザから認証情報を受け取る手段と、
- 前記認証ポリシーテーブルを用いて、前記複数のサーバから前記認証情報と適合する認証ポリシーを採用するサーバを少なくとも1つ特定する手段と、
- 前記サーバを特定する手段によって特定されたサーバの認証機構に、前記認証情報を用いてユーザ認証を行うように命令する信号を送信する手段と、
- 前記ユーザ認証が成功したことを条件として、前記ユーザの前記コンピューティング環境へのアクセスを許可する手段と、
- を備えたシステム。
- [2] 前記複数のサーバのうちの少なくとも1つの認証ポリシーの情報を取得する手段と、
- 取得した前記複数のサーバのうちの少なくとも1つの認証ポリシーを、各認証ポリシーを採用するサーバの識別子と関連付けて前記認証ポリシーテーブルに登録する手段と、
- をさらに備えた請求項1に記載のシステム。
- [3] 前記認証ポリシーテーブルを用いて、同一の認証ポリシーを採用する2以上のサーバを特定する手段と、
- 前記サーバを特定する手段によって、同一の認証ポリシーを採用すると特定された2以上のサーバの認証システム間で同一のユーザIDが登録されているかどうかを判定する手段と、
- 同一のユーザIDが登録されていると判定されたことを条件として、当該ユーザIDが同一のユーザに属するものかどうかを判定する情報を受け取る手段と、
- 前記ユーザIDが同一のユーザに属するものでないと判定されたことを条件として、当該ユーザIDを例外処理テーブルに登録する手段と、
- をさらに備えた請求項1に記載のシステム。

- [4] 新規ユーザの認証情報を受ける手段と、  
前記認証ポリシーテーブルを用いて、前記新規ユーザの認証情報と同一の認証ポリシーを採用するサーバを特定する手段と、  
前記特定されたサーバの認証システムに前記新規ユーザの認証情報と同一のユーザIDが登録されているかどうかを判定する手段と、  
同一のユーザIDが登録されていることを条件として、当該ユーザIDが同一のユーザに属するものかどうかを判定する情報を受ける手段と、  
前記ユーザIDが同一のユーザに属するものでないことを条件として、当該ユーザIDを例外処理テーブルに登録する手段と、  
をさらに備えた請求項1に記載のシステム。
- [5] 前記認証ポリシーは、文字列のユーザIDによる認証、クライアント証明書による認証、生体認証、手書き認証のうちの少なくとも一つである、請求項1に記載のシステム。
- [6] 前記アクセスを許可する手段は、前記コンピューティング環境へのアクセスを行うためのトークンを生成する手段を含む、請求項1に記載のシステム。
- [7] 前記トークンは、クッキー、URLエンコーディングによる認証情報、SAMLトークンのいずれかである、請求項6に記載のシステム。
- [8] 複数のコンピューティング環境に対する複数の認証ポリシーテーブルを備え、  
ユーザから受けた認証情報が、前記複数の認証ポリシーテーブルに登録されたサーバに適合したことに応じて、前記複数のコンピューティング環境それぞれに対してユーザ認証を行う、  
請求項1に記載のシステム。
- [9] 互いに信頼関係が確立された複数のサーバを含むコンピューティング環境における方法であって、  
前記複数のサーバのうちの少なくとも1つの認証ポリシーを登録した認証ポリシーテーブルを少なくとも1つ保持し、  
ユーザから認証情報を受けるステップと、  
前記認証ポリシーテーブルを用いて、前記複数のサーバから前記認証情報と適合

する認証ポリシーを採用するサーバを少なくとも1つ特定するステップと、

前記サーバを特定するステップにおいて特定されたサーバの認証機構に、前記認証情報を用いてユーザ認証を行うように命令する信号を送信するステップと、

前記ユーザ認証が成功したことを条件として、前記コンピューティング環境へのアクセスが許可されるステップと、

を含む方法。

- [10] 前記複数のサーバのうちの少なくとも1つの認証ポリシーの情報を取得するステップと、

取得した前記複数のサーバのうちの少なくとも1つの認証ポリシーを、各認証ポリシーを採用するサーバの識別子と関連付けて前記認証ポリシーテーブルに登録するステップと、

を含む請求項9に記載の方法。

- [11] 前記認証ポリシーテーブルを用いて、同一の認証ポリシーを採用する2以上のサーバを特定するステップと、

前記サーバを特定するステップで、同一の認証ポリシーを採用すると特定された2以上のサーバの認証システム間で同一のユーザIDが登録されているかどうかを判定するステップと、

同一のユーザIDが登録されていることを条件として、当該ユーザIDが同一のユーザに属するものかどうかを判定する情報を受けるステップと、

前記ユーザIDが同一のユーザに属するものでないことを条件として、当該ユーザIDを例外処理テーブルに登録するステップと、

を含む請求項9に記載の方法。

- [12] 新規ユーザの認証情報を受けるステップと、

前記認証ポリシーテーブルを用いて、前記新規ユーザの認証情報と同一の認証ポリシーを採用するサーバを特定するステップと、

前記特定されたサーバの認証システムに前記新規ユーザの認証情報と同一のユーザIDが登録されているかどうかを判定するステップと、

同一のユーザIDが登録されていることを条件として、当該ユーザIDが同一のユー



ザに属するものかどうかを判定する情報を受けるステップと、

前記ユーザIDが同一のユーザに属するものでないことを条件として、当該ユーザIDを例外処理テーブルに登録するステップと、

を含む請求項9に記載の方法。

[13] 前記認証ポリシーは、文字列のユーザIDによる認証、クライアント証明書による認証、生体認証、手書き認証のうちの少なくとも一つである、請求項9に記載の方法。

[14] 前記アクセスが許可されるステップは、前記コンピューティング環境へのアクセスを行うためのトークンを生成するステップを含む、請求項9に記載の方法。

[15] 前記トークンは、クッキー、URLエンコーディングによる認証情報、SAMLトークンのいずれかである、請求項15に記載の方法。

[16] (A) 前記認証ポリシーテーブル登録されている同一の認証ポリシーを採用する2以上のサーバのそれぞれに対してプライオリティを付与するステップと、

(B) 前記ユーザの認証情報が前記2以上のサーバの採用する認証ポリシーに適合したことに応じて、前記2以上のサーバのうちの前記プライオリティの最も高いサーバの認証機構に、前記認証情報を用いてユーザ認証を行うように命令するステップと、

(C) 前記ユーザ認証が失敗したことに応じて、前記2以上のサーバのうち次にプライオリティの高いサーバの認証機構に、ユーザ認証を行うように命令するステップと、

(D) 前記2以上のサーバのいずれかのサーバにおいてユーザ認証が成功するか、前記2以上のサーバすべてにおいてユーザ認証が失敗するまで、前記ステップ(C)を繰り返すステップと、

(E) 前記ユーザ認証が成功したことを条件として、前記ユーザの前記コンピューティング環境へのアクセスを許可するステップと、

を含む請求項9に記載の方法。

[17] 互いに信頼関係が確立された複数のサーバを含むコンピューティング環境におけるプログラムであって、

前記複数のサーバの少なくとも1つの認証ポリシーに登録した認証ポリシーテーブルを少なくとも1つ保持し、

前記認証プログラムは、

- ユーザから認証情報を受けるステップと、  
前記認証ポリシーテーブルを用いて、前記複数のサーバから前記認証情報と適合する認証ポリシーを採用するサーバを少なくとも1つ特定するステップと、  
前記サーバを特定するステップにおいて特定されたサーバの認証機構に、前記認証情報を用いてユーザ認証を行うように命令する信号を送信するステップと、  
前記ユーザ認証が成功したことを条件として、前記コンピューティング環境へのアクセスが許可されるステップと、  
をコンピュータに実行させるプログラム。
- [18] 前記複数のサーバのうちの1つの認証ポリシーの情報を取得するステップと、  
取得した前記複数のサーバのうちの1つの認証ポリシーを、各認証ポリシーを採用するサーバの識別子と関連付けて前記認証ポリシーテーブルに登録するステップと、  
をさらにコンピュータに実行させる、請求項17に記載のプログラム。
- [19] 前記認証ポリシーテーブルを用いて、同一の認証ポリシーを採用する2以上のサーバを特定するステップと、  
前記サーバを特定するステップで、同一の認証ポリシーを採用すると特定された2以上のサーバの認証システム間で同一のユーザIDが登録されているかどうかを判定するステップと、  
同一のユーザIDが登録されていることを条件として、当該ユーザIDが同一のユーザに属するものかどうかを判定するステップと、  
前記ユーザIDが同一のユーザに属するものでないことを条件として、当該ユーザIDを例外処理テーブルに登録するステップと、  
をさらにコンピュータに実行させる、請求項17に記載のプログラム。
- [20] 新規ユーザの認証情報を受けるステップと、  
前記認証ポリシーテーブルを用いて、前記新規ユーザの認証情報と同一の認証ポリシーを採用するサーバを特定するステップと、  
前記特定されたサーバの認証システムに前記新規ユーザの認証情報と同一のユーザIDが登録されているかどうかを判定するステップと、  
同一のユーザIDが登録されていることを条件として、当該ユーザIDが同一のユー

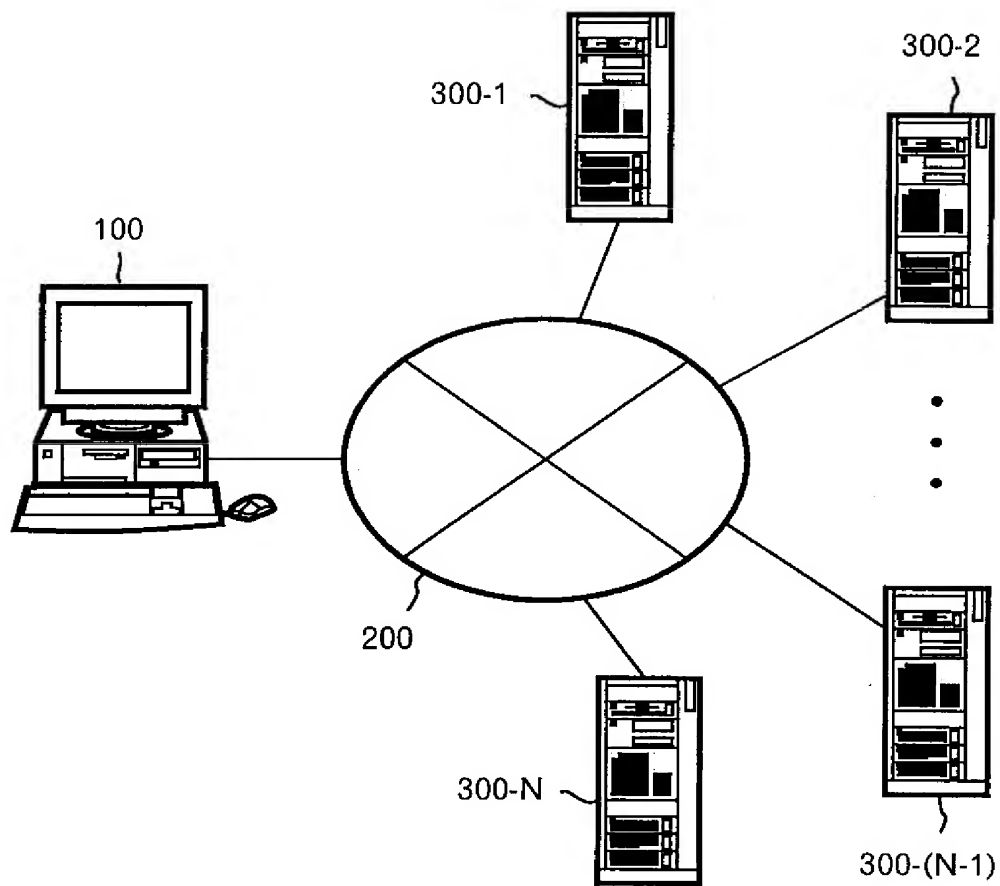
ザに属するものかどうかを判定するステップと、

前記ユーザIDが同一のユーザに属するものでないことを条件として、当該ユーザIDを例外処理テーブルに登録するステップと、

をさらにコンピュータに実行させる、請求項17に記載のプログラム。

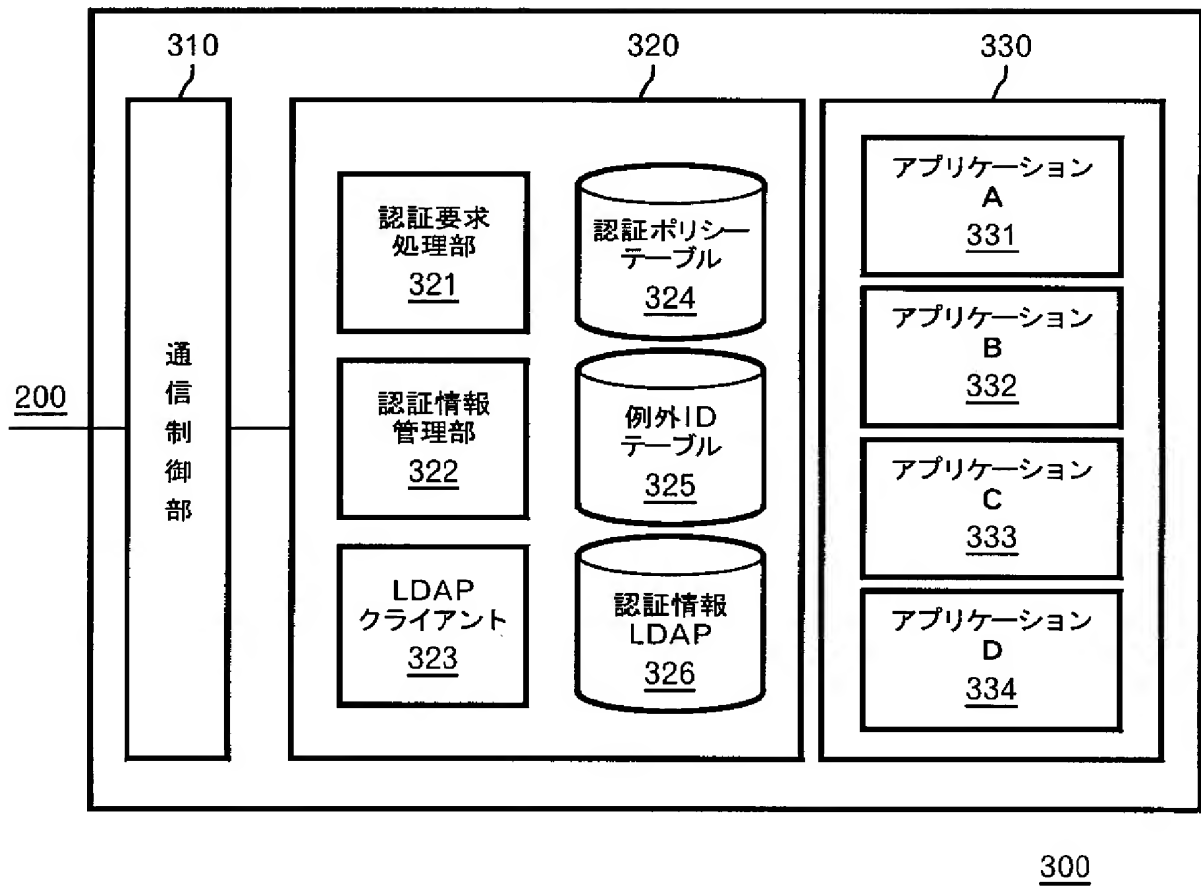
- [21] 前記認証ポリシーは、文字列のユーザIDによる認証、クライアント証明書による認証、生体認証、手書き認証のうちの少なくとも一つである、請求項17に記載のプログラム。
- [22] 前記アクセスが許可されるステップは、前記コンピューティング環境へのアクセスを行うためのトークンを生成するステップを含む、請求項17に記載のプログラム。
- [23] 前記トークンは、クッキー、URLエンコーディングによる認証情報、SAMLトークンのいずれかである、請求項22に記載のプログラム。
- [24] 請求項17ないし23のいずれかのプログラムを記録したコンピュータ可読の記憶媒体。

[図1]

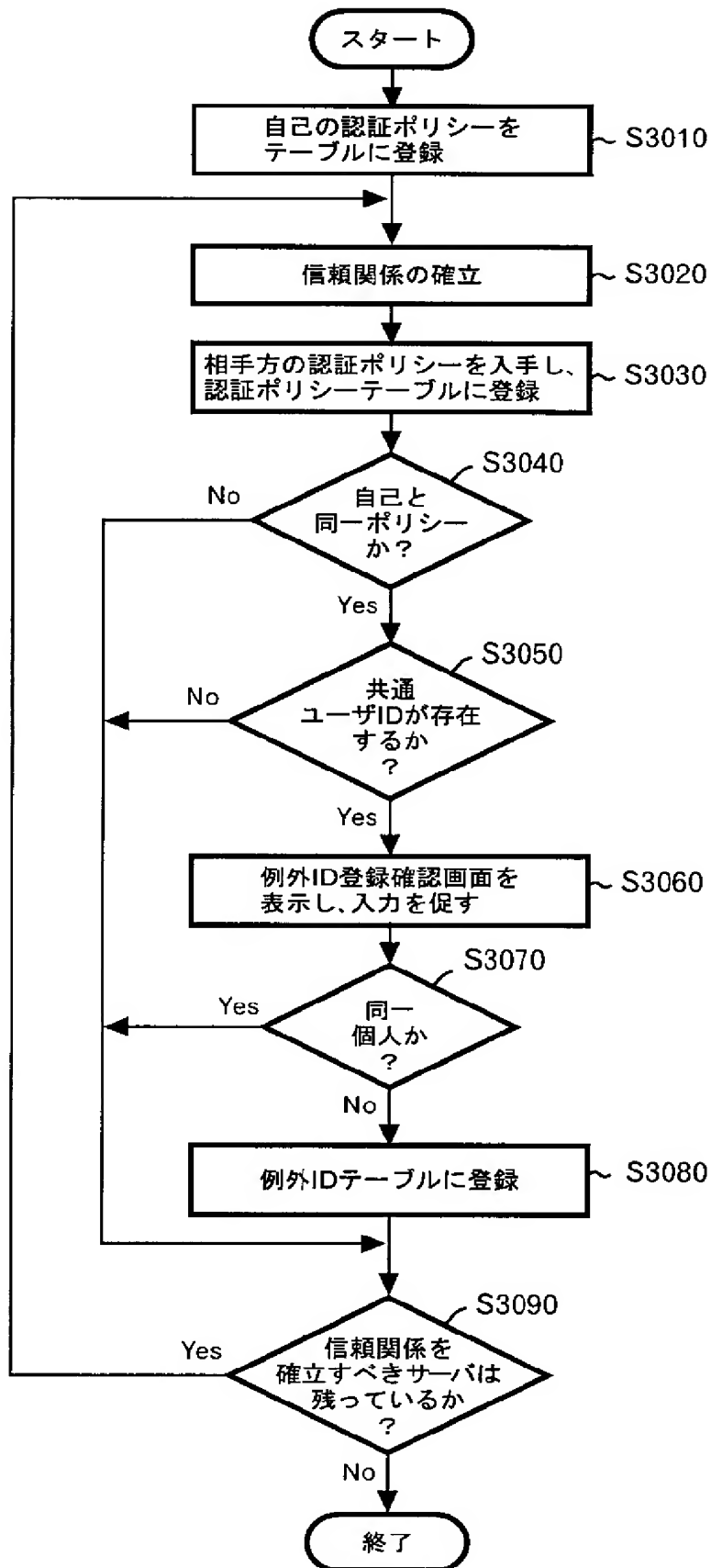


1000

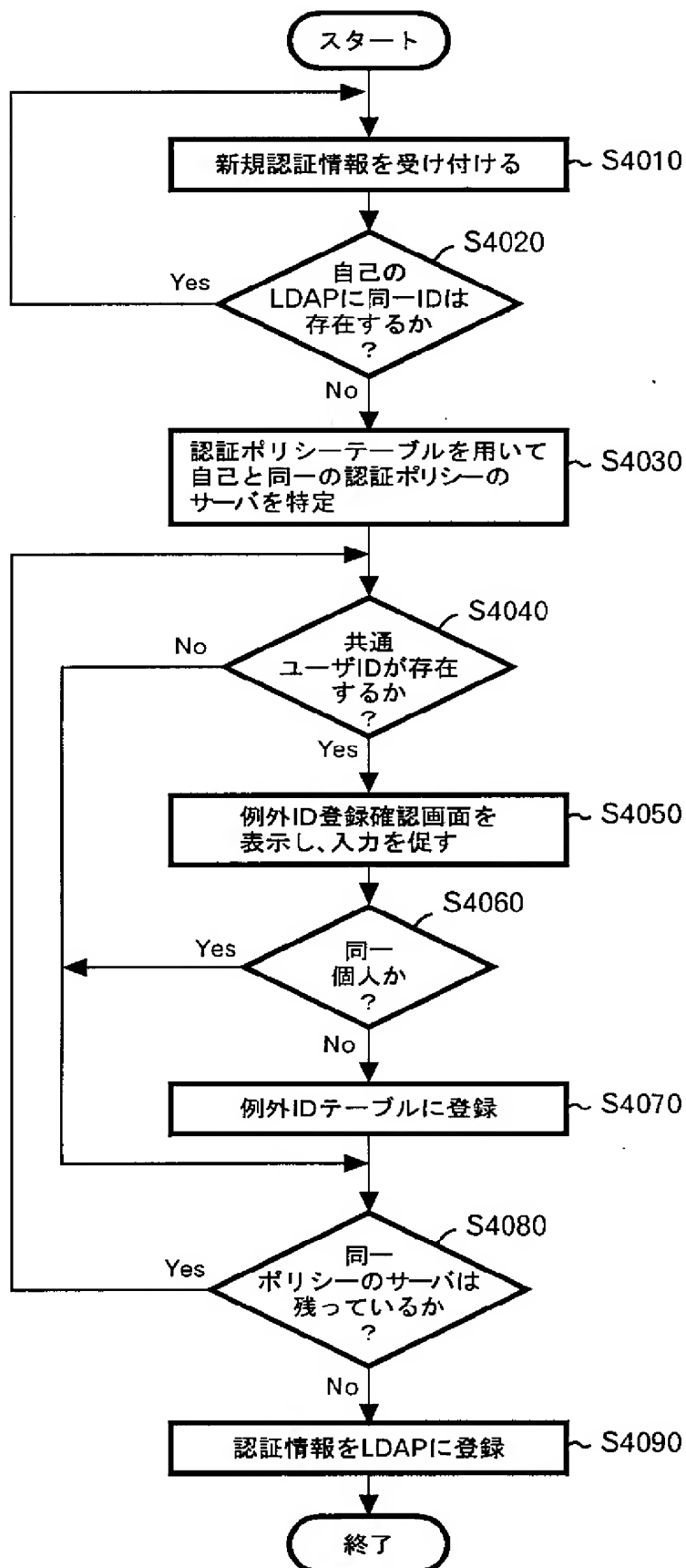
[図2]



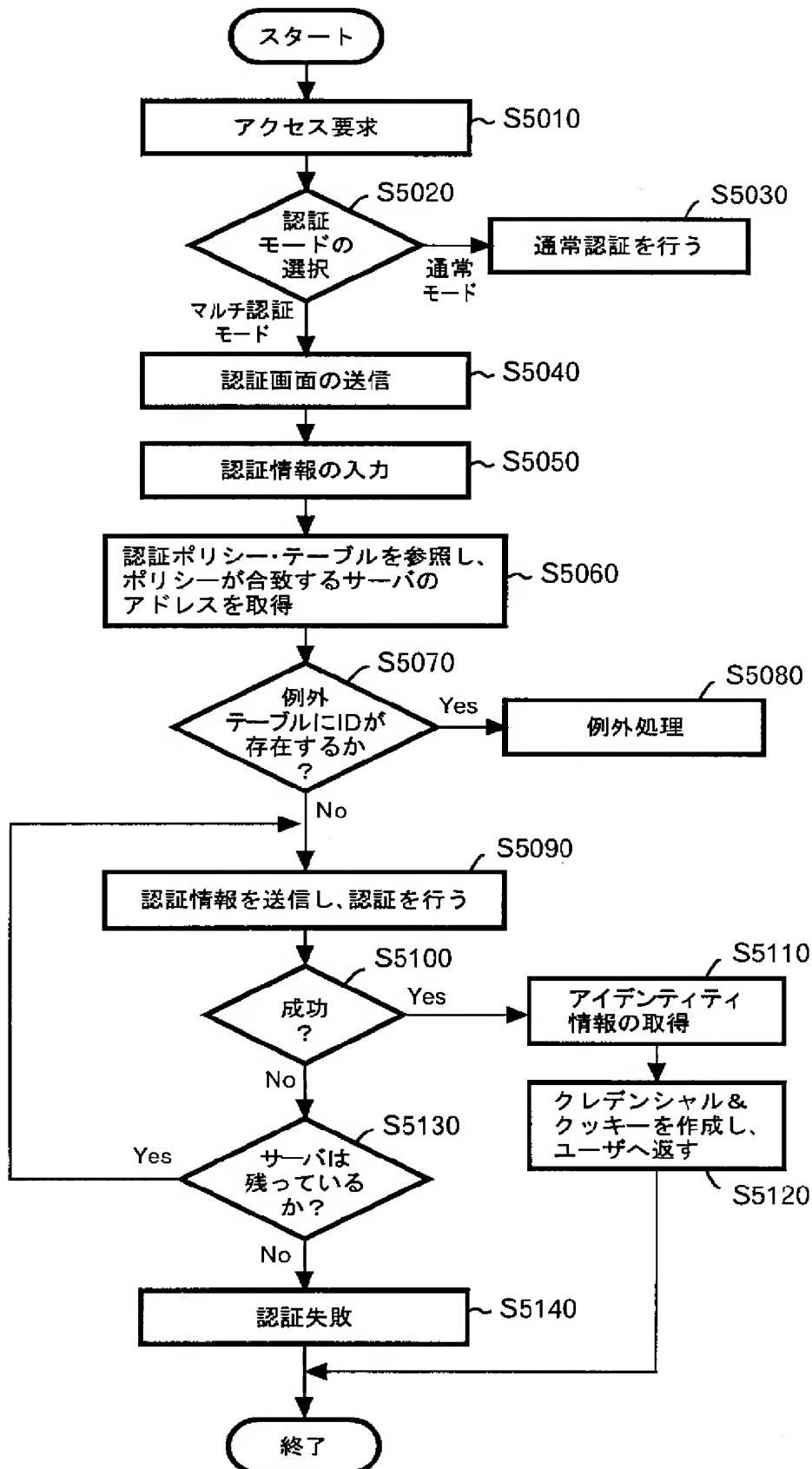
[図3]



[図4]



[図5]





[図6]



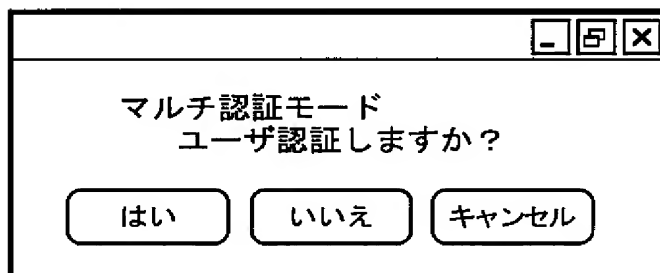
例外ID登録確認

サーバ : 300-1  
登録ユーザID : ABC001  
登録名 : Tanaka Tarou

サーバ : 300-2  
登録ユーザID : ABC001  
登録名 : Hirota Keisuke

登録する      登録しない

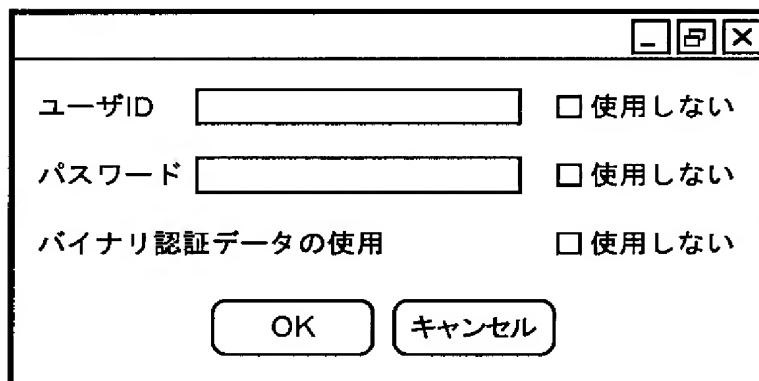
[図7]



マルチ認証モード  
ユーザ認証しますか?

はい      いいえ      キャンセル

[図8]



ユーザID  ☐ 使用しない

パスワード  ☐ 使用しない

バイナリ認証データの使用 ☐ 使用しない

OK      キャンセル

[図9]

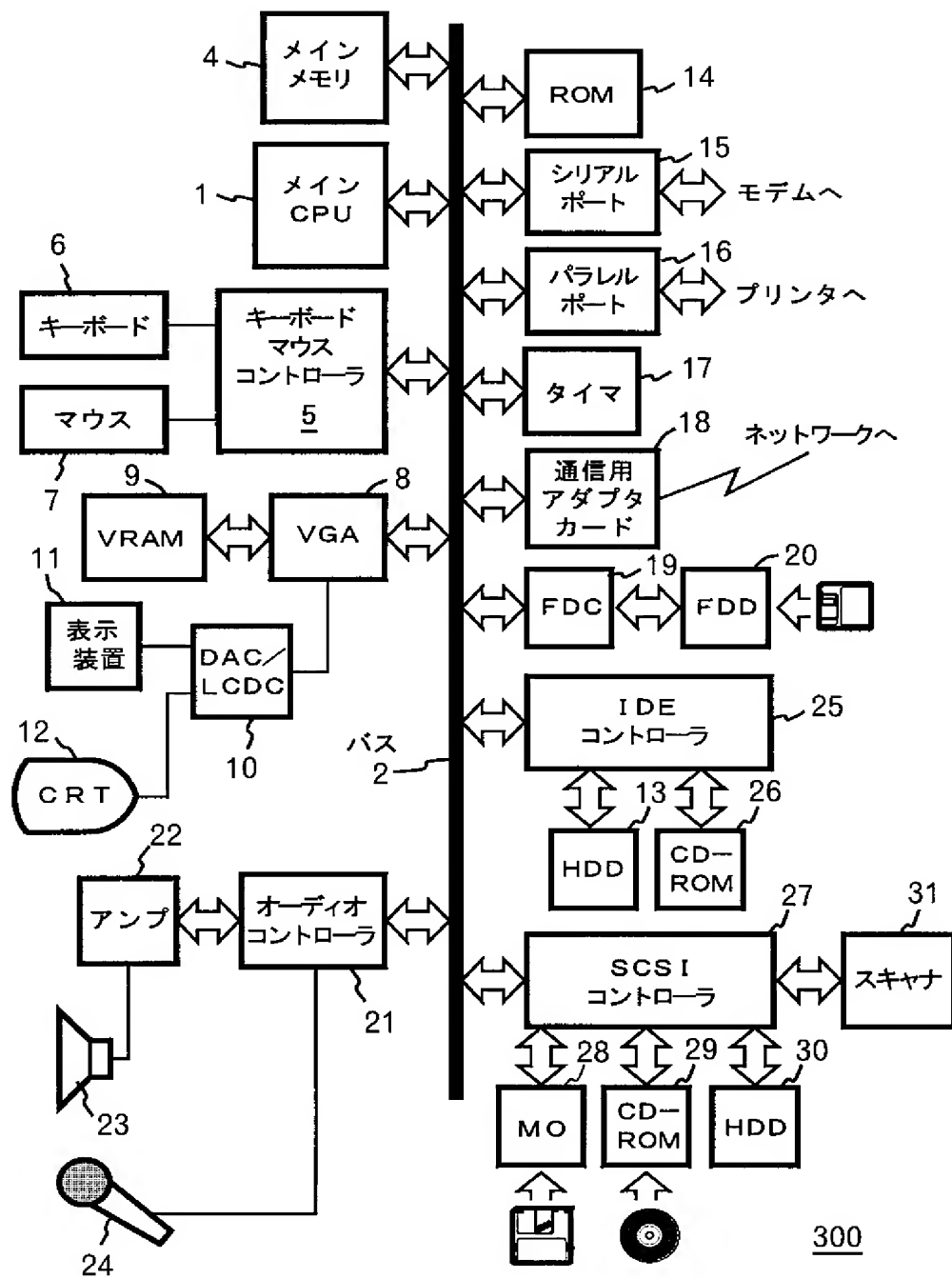
(A:アルファベット, N:数字をあらわす)

認証ポリシー	サーバアドレス	プライオリティ
ユーザID : AAANNN パスワード : AAAA	server300-1.com	1
	server300-2.com	2
	server300-3.com	3
ユーザID : AAAAAAAAA パスワード : 任意	server300-4.com	1
	server300-5.com	2
指紋認証 バイナリサイズ : 100 bytes	server300-6.com	1
	server300-7.com	2
声紋認証 バイナリサイズ : 200 bytes	server300-8.com	—

[図10]

サーバアドレス	例外ID
server300-1.com	ABC001, DEF002, GHI003
server300-2.com	ABC001, DEF002
server300-3.com	ABC001, GHI003
server300-4.com	ABCDEFGH
server300-5.com	ABCDEFGH
server300-6.com	なし
server300-7.com	なし
server300-8.com	なし

[図11]



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/002143

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F15/00, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F15/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005  
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-311138 A (NEC Corp.), 07 November, 2000 (07.11.00), Full text; all drawings (Family: none)	1, 5, 9, 13, 17, 21, 24
Y	Same as the above	6, 7, 14, 15, 22, 23
Y	JP 2000-106552 A (Hitachi, Ltd.), 11 April, 2000 (11.04.00), Full text; all drawings (Family: none)	6, 7, 14, 15, 22, 23
A	JP 2004-32311 A (NEC Corp.), 29 January, 2004 (29.01.04), Full text; all drawings & US 2003/0237004 A1	1-24

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
17 May, 2005 (17.05.05)

Date of mailing of the international search report  
31 May, 2005 (31.05.05)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/002143

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-70416 A (Ricoh Co., Ltd.), 04 March, 2004 (04.03.04), Full text; all drawings (Family: none)	1-24

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl.<sup>7</sup> G 0 6 F 1 5 / 0 0, H 0 4 L 9 / 0 0

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl.<sup>7</sup> G 0 6 F 1 5 / 0 0, H 0 4 L 9 / 0 0

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-311138 A (日本電気株式会社) 2000. 11. 07, 全文, 全図 (ファミリーなし)	1, 5, 9, 13, 17, 21, 24
Y	同上	6, 7, 14, 15, 22, 23
Y	JP 2000-106552 A (株式会社日立製作所) 2000. 04. 11, 全文, 全図 (ファミリーなし)	6, 7, 14, 15, 22, 23

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」口頭による開示、使用、展示等に言及する文献  
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」同一パテントファミリー文献

国際調査を完了した日

17. 05. 2005

国際調査報告の発送日

31. 5. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

宮司 卓佳

電話番号 03-3581-1101 内線 3546

5S

9555

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2004-32311 A(日本電気株式会社) 2004. 01. 29, 全文, 全図 & US 2003/0237004 A1	1-24
A	JP 2004-70416 A(株式会社リコー) 2004. 03. 04, 全文, 全図 (ファミリーなし)	1-24